Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1 77-9279

EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF MANAGEMENT AND BUDGET

WASHINGTON, D.C. 20503

September 23, 1977

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

Subject: Proposed policy for the security of Federal automated information systems

The attached draft memorandum supplements OMB Circular No. A-71 and provides policy guidance for developing and implementing a computer security program. Comments on the proposed policy should be forwarded to this office within 30 days. It is also requested that you provide estimates of both one-time and annually recurring resources required to implement the policy. Questions should be addressed to the Information Systems Policy Division (202) 395-4814.

Howard Messner Jr.

Wayne G. Granquist
Associate Director for Management
and Regulatory Policy

Attachment

EXECUTIVE REGISTRY FILE OMB

Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1

DRAFT
Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1

EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF MANAGEMENT AND BUDGET

WASHINGTON, D.C. 20503

Circular No. A-71
Transmittal Memorandum No. 1

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

Subject: Security of Federal automated information systems

1. Purpose. This Transmittal Memorandum promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies.

2. Background. Increasing use of computer and communications technology to improve the effectiveness of governmental programs has introduced a variety of new management problems. Many public concerns have been raised in regard to the risks associated with automated processing of personal, proprietary or other sensitive data. Problems have been encountered in the misuse of computer and communications technology to perpetrate crime. In other cases, inadequate administrative practices along with poorly designed computer systems have resulted in improper payments, unnecessary purchases or other improper actions. The policies and responsibilities for computer security established by this Transmittal Memorandum supplement those currently contained in OMB Circular No. A-71.

3. Responsibility of the heads of executive agencies. The head of each executive branch department and agency is responsible for assuring an adequate level of security for all agency data whether processed in-house or commercially. This includes responsibility for the establishment of physical, administrative and technical safeguards required to adequately protect personal, proprietary or other sensitive data not subject to national security regulations, as well as national security data. It also includes responsibility for assuring that automated processes operate effectively and accurately. In fulfilling this responsibility each agency head shall establish policies and procedures and assign responsibility for the development, implementation, and operation of an agency computer security program. The agency's computer security program shall be

Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1
DRAFT

consistent with all Federal policies, procedures, standards and guidelines issued by the Office of Management and Budget, the General Services Administration, the Department of Commerce, and the Civil Service Commission. In consideration of problems which have been identified in relation to existing practices, each agency's computer security program shall at a minimum:

a. Assign responsibility for the security of each computer installation operated by the agency, including installations operated directly by or on behalf of the agency (e.g. government-owned contractor operated facilities), to a management official knowledgeable in data processing and security matters.

b. Establish personnel security policies for screening all individuals participating in the design, operation or maintenance of Federal computer systems or having access to data in Federal computer systems. These policies should include, as appropriate, requirements for background investigations of both government and contractor personnel. Personnel security policies for Federal employees shall be consistent with policies issued by the Civil Service Commission.

c. Establish a management control process to assure that appropriate administrative, physical and technical safeguards are established for all new computer applications. While this control process should apply to all new computer applications, particular emphasis should be placed on computer applications intended to be used to issue checks, requisition supplies or perform similar functions based on programmed criteria with little or no human intervention (so-called automated decisionmaking systems). The management control process shall, at a minimum, include policies and responsibilities for:

(1) Defining and approving security specifications for all new computer applications and modifications to existing applications prior to programming such applications or changes. The views and recommendations of the computer user organization, the computer installation and the individual responsible for the security of the computer installation shall be sought and considered prior to the approval of the security specifications for the application.

(2) Conducting and approving design reviews and systems tests of new or changed computer applications prior to using them operationally. The objective of the design

reviews should be to ascertain that the proposed design meets the approved security specifications. The objective of the system tests should be to verify that the planned administrative, physical and technical security requirements are operationally adequate prior to the use of the system. The results of the design review and system test shall be fully documented and maintained as a part of the official records of the agency. Upon completion of the system test, an official of the agency shall certify that the system meets the documented and approved system security specifications, meets all applicable Federal policies, regulations and standards, and that the results of the test demonstrate that the security provisions are adequate for the application.

d. Establish an agency program for conducting periodic audits and recertifying the adequacy of the security of each operational computer application which processes personal, proprietary or other sensitive data, or which issues checks, requisitions supplies or performs similar functions with little or no human intervention (automated decisionmaking applications). This audit and recertification process is to be conducted by technically qualified professionals in an organization independent of the user organization and computer facility manager. Periodic audits and recertification shall be performed at time intervals determined by the agency, commensurate with the sensitivity of information processed and the risk and magnitude of loss or harm that could result from the application operating improperly, but shall be conducted at least every three years.

e. Establish policies and responsibilities to assure that appropriate security requirements are included in specifications for the acquisition or operation of computer facilities, equipment, software, or related services, whether procured by the agency or by the General Services Administration. These requirements shall be reviewed and approved by the management official assigned responsibility for security of the computer installation to be used. This individual must certify that the security requirements specified are adequate for the intended application and that they comply with current Federal computer security policies, procedures, standards and guidelines.

f. Assign responsibility for the conduct of periodic risk analyses for each computer installation operated by the agency, including installations operated directly by or on behalf of the agency. A risk analysis shall be performed:

Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1

(1) Prior to the approval of design specifications for new computer installations.

(2) Whenever there is a significant change to the physical facility, hardware or software at a computer installation. Agency criteria for defining significant changes shall be commensurate with the sensitivity of the information processed by the installation.

(3) At periodic intervals of time established by the agency, commensurate with the sensitivity of the information processed by the installation, but not to exceed three years, if no risk analysis has been performed during that time.

4. Responsibility of the Department of Commerce. The Secretary of Commerce shall develop and issue standards and guidelines for assuring security of automated information. Each standard shall, at a minimum, identify:

a. Whether the standard is mandatory or voluntary.

b. Specific implementation actions which agencies are required to take.

c. The time at which implementation is required.

d. A process for monitoring implementation of each standard and evaluating whether the standard is meeting its intended objectives.

e. Requirements for use of the standard in specifications for computer hardware, software or related services issued by the agency and the General Services Administration.

f. Requirements for use of the standard in specifications for the acquisition or construction of computer facilities.

g. The conditions or criteria under which waivers to the standards may be granted.

h. The procedures for granting waivers.

5. Responsibility of the General Services Administration. The Administrator of General Services shall:

Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1

a. Issue policies and regulations for the physical security of computer rooms in Federal buildings consistent with standards and guidelines issued by the Department of Commerce.

b. Assure that agency procurement requests for computers, software, and related services include security requirements which have been certified by a responsible agency official. Delegations of procurement authority to agencies by the General Services Administration under mandatory programs, dollar threshold delegations, certification programs or other so-called blanket delegations shall include requirements for agency specifications and certification of security requirements. Other delegations of procurement authority shall require specific agency certification of security requirements as a part of the agency request for delegation of procurement authority.

c. Assure that computer equipment, software, computer room construction, guard or custodial services, telecommunications services, and any other related services procured by the General Services Administration meet the security requirements established by the user agency and are consistent with other applicable policies and standards issued by OMB, the Civil Service Commission and the Department of Commerce. Computer equipment, software, or related ADP services acquired by the General Services Administration in anticipation of future agency requirements shall include security safeguards which are consistent with mandatory standards established by the Secretary of Commerce.

6. <u>Responsibility of the Civil Service Commission</u>. The Chairman of the Civil Service Commission shall establish personnel security policies for Federal personnel associated with the design, operation or maintenance of Federal computer systems, or having access to data in Federal computer systems. These policies should emphasize personnel requirements to adequately protect personal, proprietary or other sensitive data not subject to national security regulations, as well as applications which issue checks, requisition supplies or perform similar functions based on programmed criteria with little or no human intervention. Background investigations of Federal personnel should be required, as appropriate, commensurate with the sensitivity of the data to be handled and the risk and magnitude of loss or harm that could be caused by the individual.

7. <u>Reports</u>. Within 60 days of the issuance of this Transmittal Memorandum, the Department of Commerce, General Services Administration and Civil Service Commission shall submit to OMB plans for fulfilling the responsibilities specifically assigned in this memorandum. Within 120 days of the issuance of this Transmittal Memorandum, each executive branch department and agency shall submit to OMB its plans, for implementing a security program consistent with the policies specified herein.

8. <u>Inquiries</u>. Questions regarding this memorandum should be addressed to the Information Systems Policy Division (202) 395-4814.

ER
OCT 11 10 06 AM '77
1 35 PM '77
ER

STAT

Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1

Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1

	UNCLASSIFIED		CONFIDENTIAL		SECRET

Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1

EXECUTIVE SECRETARIAT

Routing Slip

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	D/DCI/IC				
4	DDS&T				
5	DDI				
6	DDA	X			
7	DDO				
8	D/DCI/NI				
9	GC				
10	LC				
11	IG				
12	Compt	[illegible]	✓		
13	D/Pers				
14	D/S				
15	DTR				
16	Asst/DCI				
17	AO/DCI				
18	C/IPS				
19	DCI/SS				
20	D/EEO				
21					
22					

SUSPENSE ______ Date

Remarks:

Direct response.

STAT

Executive Secretary

30 Sep

Date

Approved For Release 2004/03/31 : CIA-RDP80M00165A002100050006-1

3637 (7-76)